U.S. National Stage Patent Application of Manfred Blumberg, et al.
Attorney Docket No. 7701-0002WOUS
Claiming priority to PCT/EP2003/011569
filed 10/17/03

METHOD AND DEVICE FOR PREVENTING A CONTROL ERROR OF A MACHINE TOOL

"EXPRESS MAIL" MAILING LABEL
NUMBER EV 713350392 US
DATE OF April 12, 2006
I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 C.F.R. 1.10 ON THE DATE INDICATED ABOVE AND IS ADDRESSED TO THE COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450

Christine Rounds
(TYPED OR PRINTED NAME OF PERSON MAILING PAPER OR FEE)

Christine Rounds
(SIGNATURE OF PERSON MAILING PAPER OR FEE)

Title: Machine tool protected against improper activation and method of avoiding improper machine activation by machine control parameters for this

[0001] The present invention relates to a machine tool protected against improper activation and an associated method of avoiding improper machine activation by machine control parameters.

[0002] Against the background of increasingly interlinked production processes and their standardization in the industry, the problem that is nowadays the prime concern in the production of machine tools is that of also incorporating in this process the computer systems that are necessary for activating the machine tools. In this respect, one aim is to provide, to the extent technically possible, standardized machine control systems, offering the user greatest possible uniformity of the machine control parameters for the products from his range of workpieces - for instance when changing an actual machine type or else for improved data storage and archiving.

[0003] Such initiatives have already been pursued for some time for various types of machine tool.

[0004] For bevel gear cutting machines there are for instance solutions to this in which the relevant machine control parameters of an entire machine family are combined in a standardized data model with all the axes to be activated that come into consideration in the machine family, which then, in individual cases, is replicated on the respective machine actually concerned - to the extent to which this is possible, that is to say the axes activated by the machine control parameters are also actually present.

[0005] One problem of these systems is, however, that the standard data model created by them for the machine control parameters also entails great risks for the operational reliability of the machine tools respectively activated with them. While in the case of a non-standard data model there is no risk of using the

machine control parameters to activate a machine type which is not suitable for these parameters, because it cannot even read the corresponding format, or at least not process it, this is no longer ruled out in the case of the standardization mentioned above. Rather, here it is the case that all the machine types can read in the machine control parameters in their standard format and also process them for their control; however, here it is not ensured that this processing then always leads to an appropriate working result on the machine. Indeed, more troubling still, it is still possible for machine control parameters which have been generated for one machine type 1 to be incorrectly sent to a machine of type 2, which then processes them and thereby controls its axes in such a way as to cause irreparable damage to the machine itself or even personal injury, for instance as a result of electric cables being severed by cutting tools improperly controlled in this way.

[0006] Such improper activation can be avoided for instance by adding to the machine control parameters a machine address, which specifies the machine that can be activated with the aid of the machine control parameters, and by setting up the machines in such a way that they first check from this added machine address whether the machine control parameters are also actually suitable for them. Such a procedure presupposes, however, that the machine control parameters protected in this way are also actually in an unchanged form when they reach the machine from the source from which they originate. This cannot always be ensured, however. Rather, it is the case that, once generated, parameters of this type are easy to change. For instance, it is possible that machine control parameters are generated for a specific workpiece and a specific machine, but this machine is not available at the planned production time. If another machine is provided instead, one which is capable in principle of

processing the machine-independent format of the machine control parameters, but for different limit values and under different boundary conditions in terms of safety than those which apply to the machine originally planned for use, there is a great temptation simply to use the machine control parameters for this machine although they are not enabled for it, in that, instead of the original machine address of the machine that is not available, now the address of the other machine, which although available for these control parameters has not been enabled, is entered - for instance by means of an editor.

[0007] Experience shows that, in today's production plants, which are under strong pressure to produce results, such a procedure breaching safety functions is not uncommon.

[0008] It is therefore the object of the present invention to provide a machine tool which is protected against improper activation and associated methods of avoiding improper machine activation by machine control parameters which ensure to the greatest extent possible that control parameters once generated for a specific machine are also only used for activating this machine.

[0009] This object is achieved according to the invention by a machine tool protected against improper activation which has an open-loop and/or closed-loop control device for the activation of machine functions, preferably machine axes, and means for reading in machine control parameters for the open-loop and/or closed-loop control device from a data carrier or electronic carrier signal, which is characterized in that it has an improper-activation safety module, preferably an improper-activation safety software module, which decodes the machine control parameters again that are intended for the machine tool and are encoded by means of an asymmetric encryption method,

using an encryption key which is assigned to the machine tool and provided for the encryption, with the aid of a decryption key which is likewise assigned to the machine tool, is different from the encryption key and is provided for the decryption, and which module enables the machine control parameters for controlling the machine tool only in the case of successful decryption.

[0010] Also helping to achieve this object is a data carrier according to the invention or an electronic carrier signal with machine control parameters for reading into the machine tool, the data carrier or the electronic carrier signal having on it machine control parameters for the machine tool which are encoded by means of an asymmetric encryption method with the aid of an encryption key which is assigned to the machine tool and is provided for the encryption, so that the machine tool can decode them again with the aid of a decryption key which is likewise assigned to it, is different from the encryption key and is provided for the decryption, and the data carrier or the electronic carrier signal controls the machine tool by means of these machine control parameters during reading-in or after reading-in after they have been decoded.

[0011] Similarly helping to achieve the object according to the invention is a method of avoiding improper machine activation by machine control parameters of a machine tool in which the machine control parameters intended for the machine tool are encoded by means of an asymmetric encryption method with the aid of an encryption key which is assigned to the machine tool and is provided for the encryption, so that the machine tool can decode the machine control parameters again with the aid of a decryption key which is likewise assigned to it, is different from the encryption key and is provided for the decryption.

[0012] The aforementioned machine tool according to the invention, the data carrier or carrier signal according to the invention with machine control parameters for reading into the machine tool and also the associated method according to the invention of avoiding improper machine activation by machine control parameters now achieve the effect that only the machine for which the machine control parameters were generated is activated, in that only this machine is capable in the first place of decrypting the data intended for it and encoded with an encryption key assigned to it, and then subsequently processing the said data. For this purpose, a method already known from the prior art (for instance from Bauer, Friedrich L., Entzifferte Geheimnisse - Methoden und Maximen der Kryptologie [deciphered secrets - methods and maxims of cryptology], Berlin Heidelberg 1995, pages 153-168, or Diffie, W. and Hellman, M.E., New Directions in Cryptography, Transactions IEEE Inform. Theory, IT-22, 6 (1976), 644 - 654 or else US 4,405,829, all texts of which the disclosure content is expressly incorporated here by way of reference), namely a so-called asymmetric encryption method, is used - although here in an extremely unusual way - in which a message for a recipient is encoded by means of an encryption key (also referred to in the literature as a public key), which message can then be decoded again by the said recipient by means of a decryption key which is different from the public key and in the literature is also referred to as a so-called private key. According to the present invention, this method is used, however, in such a way that the encryption key does not serve for encoding, i.e. making a message unreadable, but rather for the secure addressing of the correct recipient. In other words, the encryption key acts here both as a security mechanism against unauthorized manipulations of the machine control parameters encrypted with it and also inherently, by way of the asymmetric encryption method used, as a machine address

of the associated machine tool. By contrast with the object of an asymmetric encryption method according to the prior art, here it is not the aim to keep the machine control parameters secret in some way, but only to make certain that the parameters are only used to activate the machine that can also ensure operationally reliable execution of these control instructions. This is also reflected in the use of the encryption and decryption keys. This is so because in the present invention it is precisely the encryption key, referred to in the prior art as public (known as the 'public key', see above), that is the actual 'secret' key, i.e. known only to the authorized system for the generation of machine control parameters; without knowledge of this encryption key, a machine cannot be activated by means of generated machine control parameters. Conversely, the decryption key referred to in the prior art as the 'private key' does not necessarily have to be kept secret according to the present invention. Rather, it can be used publicly, for instance for making the communication traffic between a computer system for generating the machine control parameters and the respective machines transparent, without the aim pursued by the invention of operationally reliable machine activation being put at risk as a result.

[0013] If, however, other considerations make it desirable for the decryption key of the machine tool also to be kept secret, it is recommendable to use an embodiment of the machine tool according to the invention in which the latter has a reader, preferably a chip card reader, which is intended for receiving a decryption module, preferably a chip card, which has the decryption key, with the aid of which the improper-activation safety module decodes the encoded machine control parameters, and the decryption module being set up in such a way that only the improper-activation safety module can read out the decryption key from the module, which can easily be achieved for instance by

the data that are located in the module, that is also the decryption key itself, in turn being encoded, the improper-activation safety module having the key for the decryption of the module data.

[0014] The determination whether a decryption was successful can preferably happen by taking place after the decryption on the basis of finding a machine identification assigned to the machine tool, the associated method according to the invention of avoiding improper machine activation by machine control parameters of a machine tool according to the present invention being designed in such a way that a machine identification assigned to the machine is added to the machine control parameters before the encryption, so that, when it decodes the machine control parameters again with the aid of its assigned private decryption key, the machine tool can determine on the basis of the fact that these contain the machine identification assigned to it that the parameters concerned are machine control data for its activation. The corresponding data carrier or the corresponding electronic carrier signal with machine control parameters for reading into the machine tool is in this case designed in such a way that on the data carrier or the electronic carrier signal there is at least one machine identification included in the encryption and assigned to the machine tool, so that, when it decodes the machine control parameters again with the aid of its assigned private decryption key, the machine tool can determine on the basis of the fact that these contain the machine identification assigned to it that the parameters concerned are machine control data for its activation.

[0015] In a particularly preferred embodiment, the machine tool according to the invention, protected against improper activation, is characterized in that the improper-activation safety module enables various

functions of the machine tool for control by the machine control parameters in dependence on the decryption key originating from a plurality of decryption keys assigned to the machine tool.

[0016] Nowadays it is often the case that, in respect of its physical component parts, one and the same machine is offered on the market in variants which differ both in price and in function. The individual variants thereby often differ only in different control modules, preferably software modules, or even only in the different enablement by the manufacturer of different (software) modules already present in the machine, according to which options the customer is prepared to pay for. The present invention is ideally suited in the embodiment described above for also ensuring this functionality largely with security with respect to manipulations, in that modules, preferably software modules, with a differing functional extent are stored in the machine and are respectively assigned different encryption and decryption keys. The customer acquiring a specific machine variant is then also always supplied at the same time with the encryption key - coded openly, or if desired also in a concealed manner (for instance a chip card as stated above) -, which serves as an inherent machine address of the module corresponding to the extent of performance he has ordered. The machine control parameters encoded by means of this encryption key can then only be decrypted and further processed by this module. All other modules, on the other hand, cannot do anything with the parameters. In practice, this can be realized for instance by all the modules attempting one after the other to decrypt the machine control parameters until finally one (or even none) is successful, it also being possible for this procedure to be optimized by always beginning with the module that was last successful in decryption in all further attempts at decryption, so that processing time is saved as a result, and a new

module is sought only in the case of changing the encryption key, serving as it were in this way as an address of a virtual machine - for instance in the event of a so-called upgrade. In this connection, it is to be emphasized that the present invention is particularly suitable for upgrades of this type, in that in such a case the customer wishing to acquire new options for his machine is simply correspondingly provided with new decryption or encryption modules, preferably chip cards, which represents a solution which is decidedly secure with respect to manipulations and cost-effective.

[0017] A further preferred embodiment of a machine tool according to the invention, protected against improper activation, is distinguished by the fact that the improper-activation safety module determines successful decryption of the machine control parameters after decryption also on the basis of finding a signature of a unit authorized for activating the machine tool.

[0018] The associated method of avoiding improper machine activation by machine control parameters of a machine tool according to the present invention is characterized in that the machine control parameters intended for the machine tool are first encoded by means of a private decryption key, assigned to the sender of the machine control parameters, and are provided with a sender identification of this sender, and, signed by the sender in this way, are only encoded with the aid of the encryption key that is assigned to the machine tool and known for the encryption.

[0019] Signature methods are methods which serve for the authentication of a message with regard to it sender. Asymmetric encoding methods can also be used as signature methods whenever the message can be both decoded with the decryption key when it has been

encoded with the encryption key and decoded with the encryption key when it has been encoded with the decryption key (cf. also in this respect for instance the texts already incorporated here in the disclosure content by reference, for instance from Bauer, Friedrich L., Entzifferte Geheimnisse - Methoden und Maximen der Kryptologie, Berlin Heidelberg 1995, pages 153-168, in particular pages 155 and 156 therein, or else US 4,405,829). In such a signature method with an encryption key and a decryption key of the sender, the latter can then sign a message in a way which can easily be checked, in that the sender initially encodes the message with his decryption key, then adds a sender identification to this key and encodes the overall message created in this way with the encryption key belonging to the target machine. After decoding, this machine can then initially read the sender identification and determine by means of this - for instance on the basis of a directory, such as a list or a data bank -, which encryption key is assigned to this sender identification. If then - on the basis of the special additional characteristic of this asymmetric encoding system explained at the beginning of this section - this encryption key found in this way is suitable for the decryption of the message, the machine knows that the message actually comes from the sender corresponding to the identification used in the overall message.

[0020] In the present case, such a signature method that is already known from the prior art can thus be additionally used not only for checking on the machine tool whether the machine control parameters were actually generated for this machine, but also for determining whether the system which generated the data - that is the sender in the terminology used above - is also actually suitable and authorized to do so, for instance on the basis of a corresponding list. If this is not the case, in this embodiment the machine does

not process the corresponding machine control parameters. Such an embodiment consequently offers the possibility of certifying systems for the generation of machine control parameters and enabling them for the activation of machine tools. In this way it is possible to prevent for instance that those systems which do not offer sufficient assurance for the security of the often highly complex activation of the machine with its axes are excluded from the activation of the machines.

[0021] Also serving here for the operation of the machine tool according to the invention is preferably a data carrier according to the invention or an electronic carrier signal according to the invention with machine control parameters for reading into the machine tool, the data carrier or the electronic carrier signal having on it machine control parameters for the machine tool which are first encoded by means of a private encryption key, assigned to the sender of the machine control parameters, and are provided with a sender identification of this sender, and, signed in this way, are only encoded with the aid of the encryption key that is assigned to the machine tool and known for the encryption.

[0022] Also serving for carrying out the present invention is a method of generating machine control parameters for a machine tool which is characterized according to the invention in that it generates a data carrier or an electronic carrier signal with machine control parameters as described above. It goes without saying that this method may also to be realized on a computer system with at least one data processing unit and at least one memory, usually for instance as a computer program, it having the corresponding instructions set up for carrying out the method. Such a computer program may in this case take any form, but in particular also that of a computer program product

on a computer-readable medium, such as for instance a floppy disc, CD or DVD, it having computer program coding means, with which, after loading the computer program, a computer is in each case made by the program to carry out the method of generating a data carrier or electronic carrier signal according to the invention. It may, however, also be for instance in the form of a computer program product which has a computer program on an electronic carrier signal, with which, after loading the computer program, a computer is in each case made by the program to carry out the method according to the invention.

[0023] In the same way as described above, the method according to the invention may be used to avoid improper machine activation by machine control parameters of a machine tool in all embodiments on a correspondingly set up computer system. It may take the form of a computer program, for instance on a data carrier or an electronic carrier signal, for instance for downloading. A computer system set up in this way for generating machine control parameters for a machine tool according to the invention may in this case also have a reader, preferably a chip card reader, which is intended for receiving an encryption module, preferably a chip card, which has the encryption key, with the aid of which the computer system encodes the machine control parameters, and furthermore an encoding module, preferably an encoding software module, is provided for encoding the machine control parameters, the encryption module being set up in such a way that only the encoding module can read out the encryption key from the module. It should be additionally noted at this point that of course all other further data necessary for the present invention can be stored completely or partly on a module allowing reading out, for instance the decryption module or the encryption module, preferably in such a way that they are secured against unauthorized reading out. All these embodiments which

use such modules, preferably chip cards, offer the advantage that they can be configured extremely flexibly with the aid of an external system, without requiring any modification of the software in the respective machine tool or the respective computer system for generating the control parameters.

[0024] The different individual elements of the present invention described above, seen in their entirety, can provide a computer control system for avoiding improper machine activation by machine control parameters for a machine tool with

- a computer system for generating machine control parameters for a machine tool according to the invention or

- a computer program or computer program product for this, and

- at least one machine tool according to the invention.

[0025] Further details of such a system according to the present invention can be taken from the exemplary embodiments.

[0026] Exemplary embodiments of the present invention, which are to be understood as non-restrictive, are discussed below on the basis of the drawing, in which:

[0027] Figure 1 shows a computer control system according to the invention for avoiding improper machine activation by machine control parameters for a machine tool.

[0028] Figure 1 shows a computer control system according to the invention for avoiding improper

machine activation by machine control parameters for a machine tool, to be precise with a computer system 1 according to the invention for generating machine control parameters for a machine tool 2, 2a according to the invention with at least one data processing unit and at least one memory, the data processing unit being set up in programming terms in such a way that it generates here in a data network an electronic carrier signal 3 with machine control parameters according to the present invention, and two machine tools 2, 2a according to the invention.

[0029] In the present case, the situation is therefore such that the first machine 2 has (along with other axes) a mechanical pivoting axis σ_1 for the pivoting of the workpiece and the grinding wheel with respect to each other by means of a rotation of the grinding wheel axis or its parallel projection in the horizontal plane A. The second machine 2a likewise has such a pivoting axis σ_2, but, on account of further mechanical components in the pivoting range of this axis, cannot cover the complete pivoting angle of the pivoting axis σ_1, even though this second machine 2a can in principle, on account of the same basic construction, in fact still activate the pivoting axis of an entire angular range, which from a certain position, however, then leads to breakage. The present invention now offers the possibility of effectively preventing operation involving such breakage. The machine 2 with the greater pivoting angle has an improper-activation safety software $module_{M2}$, with associated encryption key_{M2} and decryption key_{M2}. The second machine 2a with the smaller pivoting angle contains its own improper-activation safety software $module_{M2a}$, with associated encryption key_{M2a} and decryption key_{M2a}. The computer system 1, which generates the machine control parameters, then knows which maximum angle is available for activation to the respective machine 2, 2a for the mechanical pivoting

axis σ_1, σ_2. In order that machine control parameters for the first machine 2 are then not mistakenly used on the other machine 2a, they are encrypted by means of an encryption module C, preferably a software module, by means of the respective encryption key, namely the encryption key_{M2} or else the encryption key_{M2a}, as the respective inherent address of the associated machine, this key being read in from a chip card 4 by means of a corresponding reader. In this way it is thus ensured that only the machine 2, 2a addressed by means of this key is also actually activated by the machine control parameters, and so breakage does not occur, since the respective machine 2, 2a can also only read the control parameters addressed to it by means of their respective improper-activation safety software module and the decryption key read in from their own chip card 4a, 4b by means of a reader.

[0030] In order that the respective machine 2, 2a can also make certain that the control parameters also actually originate from a source which is capable of ensuring reliable activation of the machine 2, 2a, here the machine control parameters are also signed by means of a signature method using a sender identification. With the aid of an encryption key and a decryption key of the sender, namely with the aid of the keys encryption key_{Comp1} and decryption key_{Comp1}, the machine control parameters can be signed by the computer system 1 in a way which can easily be checked, in that it, as the sender, initially encodes the control parameters with its decryption key_{Comp1}, then adds the sender identification to this key and encodes the overall message created in this way with the encryption key_{M2} or encryption key_{M2a} belonging to the target machine 2, 2a. After decoding, the respective machine 2, 2a can then initially read the sender identification, here sender $identification_{Comp1}$, and determine by means of this - here on the basis of a directory on the chip card 4a, 4b -, which encryption key is assigned to this sender

identification, here encryption key_{Compl}. If then, on the basis of the special additional characteristic of this asymmetric encoding system that is required and used here in the general part of the description (as for instance in the case of the known RSA method, cf. also US 4,405,829), this encryption key found in this way is suitable for the decryption of the message, because it was encrypted by means of the decryption key, the machine 2, 2a knows that the message actually comes from the computer system 1 as the sender corresponding to the identification used in the overall message, sender $identification_{Compl}$. The fact that this identification is recorded on the chip card 4a, 4b allows the machine to rely on the suitability of the sender for activation.